(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer: **0 631 408 A2**

(12) # EUROPÄISCHE PATENTANMELDUNG

(21) Anmeldenummer: **94106983.3**

(51) Int. Cl.[5]: **H04L 9/32**

(22) Anmeldetag: **04.05.94**

(30) Priorität: **25.05.93 DE 4317380**

(43) Veröffentlichungstag der Anmeldung:
28.12.94 Patentblatt 94/52

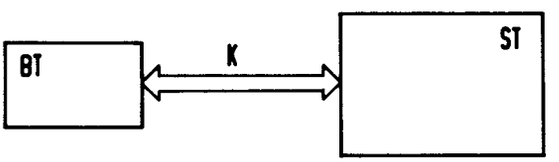
(84) Benannte Vertragsstaaten:
AT BE CH DE DK ES FR GB GR IE IT LI NL PT SE

(71) Anmelder: **SIEMENS AKTIENGESELLSCHAFT**
Wittelsbacherplatz 2
D-80333 München (DE)

(72) Erfinder: **Eberhard, Günther, Dipl.-Phys.**
Herbststrasse 45
D-82223 Eichenau (DE)

(54) **Verfahren zur Authentifikation zwischen zwei elektronischen Einrichtungen.**

(57) Das Verfahren zur Authentifikation weist folgende Schritte auf:
Generieren wenigstens zweier Zufallszahlen. Übermitteln der beiden Zufallszahlen, so daß beide in beiden Stationen zur Verfügung stehen. Verschlüsselung der Zufallszahlen in beiden Stationen zu jeweils einen jeder Zufallszahl zugehörigen Kryptogramm.Übersenden eines Teils des ersten Kryptogramms von einer Station an die andere Station. Vergleich des Kryptogrammteils in der anderen Station und bei Nichtübereinstimmung Abbruch der Ausgabe des restlichen Kryptogramms. Übersenden eines Teils des zweiten Kryptogramms von der anderen Station. Vergleich des von der anderen Station gesendeten Kryptogrammteils in der einen Station und Abbruch des restlichen Kryptogramms bei Nichtübereinstimmung. Wiederholung der Schritte d) bis g) mit den weiteren Teilen des Kryptogramms bis vollständige Übereinstimmung vorliegt oder Abbruch erfolgte.



EP 0 631 408 A2

Die Erfindung betrifft ein Verfahren zur Authentifikation zwischen zwei elektronischen Einrichtungen, wie z. B. Datenstationen.

Ein derartiges Verfahren ist z.B. aus der US-3 761 892 bekannt. Bei einem derartigen System werden von einer Station Daten an die andere Station übermittelt, daraufhin wird von der anderen Station das Datum mit einem Codeschlüssel zu einem Kryptogramm verschlüsselt und schließlich zurück an die erste Datenstation gesendet. Diese überprüft, ob das Kryptogramm richtig ist, d. h. ob der von der einen Station bekannte Codeschlüssel verwendet worden ist, und damit die Datenstation zugangsberechtigt ist.

In der US 3,761,892 ist beschrieben, daß es höchst wünschenswert ist, daß das System inoperativ bleibt, solange bis der komplette Datensatz/Kryptogramm übertragen worden ist, auch wenn bereits der erste Teil oder auch ein anderer Teild des Kryptogramms nicht mit einem zulässigen Kryptogramm übereinstimmt. Eine derartige Vorgehensweise ist bei diversen Datenstationen sicherlich sinnvoll, jedoch bei z.B. tragbaren Chipkarten kann eine derartige komplette Übertragung des Kryptogramms dazu führen, daß ein nicht legitmierter Benutzer mit einer gültigen Karte die Übertragung von Autentifikationsvorgängen mittels geeigneter Einrichtungen beobachtet und anhand der ermittelten Daten eine gültige Karte letztendlich simulieren kann.

Aufgabe der vorliegenden Erfindung ist es ein Verfahren anzugeben, welches die Nachbildung durch einen Betrüger wesentlich erschwert.

Diese Aufgabe wird durch die Verfahrensschritte des kennzeichnenden Teils des Anspruchs 1 gelöst. Weiterbildungen sind Kennzeichen der Unteransprüche.

Vorteil der Erfindung ist es, daß bei der erfindungsgemäßen in wechselseitigen Schritten vorzunehmenden Authentifikation zwischen den elektronischen Einrichtungen im Fall eines versuchten Angriffs durch Nichtübereinstimmung der zu vergleichenden Einzelschrittinformationen bereits zu Beginn des Vorgangs eine weitere Ausgabe gesperrt werden kann und damit dem Angreifer keine nutzbringenden Daten bekannt gemacht werden. Dadurch erhöht sich die Wahrscheinlichkeit, daß durch ein erzwungenes Protokoll, bei dem mit großer Sicherheit bereits nach wenigen Versuchen der Authentifikationsvorgang bereits abgebrochen werden kann und auch die Benutzung der Karte gesperrt werden kann, keine für Fälschungen wichtige Informationen preisgegeben werden.

Ein weiterer Vorteil des erfindungsgemäßen Verfahrens ist daß die Authentifikation mit relativ geringem Aufwand erfolgen kann und dadurch keine allzu hohe Rechenleistung für die Datenstationen erforderlich ist, da ein wesentliches Angriffspotential entfällt. Dies erweist sich auch als besonders vorteilhaft bei der Verwendung einer Chipkarte als eine Datenstation.

Figur 1 zeigt eine Anordnung mit zwei Datenstationen BT, ST und einer Kopplungseinrichtung K zur Datenübertragung zwischen den Datenstationen. Eine derartige Anordnung ist sowohl bei bisherigen Authentifikationsverfahren wie auch bei dem erfindungsgemäßen verwendbar.

Nachfolgend wird das konventionelle Verfahren zur Authentifikation am Beispiel der Übertragung zwischen einem beweglichen Datenträger BT und einer stationären Schreib/Lesestation ST erläutert: Zuerst generiert die stationäre Station ST eine Zufallszahl R und sendet diese Zufallszahl R über die Ankopplungsmittel K an den beweglichen Datenträger BT, der z.B. eine Chipkarte sein kann. Anschließend verschlüsselt die stationäre Station ST die Zufallszahl R mit einem Geheimschlüssel GS. Der bewegliche Datenträger BT empfängt die Zufallszahl R und verschlüsselt sie mit dem Geheimschlüssel GS der ebenfalls auf dem beweglichen Datenträger BT gespeichert ist. Das so erhaltene Kryptogramm wird dann wiederum über die Kopplungsmittel K an die stationäre Station ST gesendet. Die stationäre Station ST empfängt das Kryptogramm und vergleicht dieses mit dem eigenen berechneten Kryptogramm. Bei Übereinstimmung wird der bewegliche Datenträger als echt erkannt.

Umgekehrt kann ein analoges Verfahren zur Authentifikation des Terminals erfolgen, hier wird jedoch das Kryptogramm der stationären Station an den beweglichen Datenträger gesendet und der Vergleich erfolgt im beweglichen Datenträger.

Wie bereits zuvor beschrieben, kann bei der angegebenen Reihenfolge der gegenseitigen Authentifikation der bewegliche Datenträger durch eine Abfrageelektronik, z.B. ein falsches Terminal, zur Ausgabe eines einer eingegebenen Information zugeordneten Kryptogramms veranlaßt werden. Bei aus Aufwandsgründen kleinen Schlüssel kann hieraus ein Angreifer durch Durchvariation der Schlüssel den zugeordneten Geheimschlüssel bestimmen. Hierbei handelt es sich um einen sogenannten gewählten Klartext-Angriff. Wird die Reihenfolge der Authentifikation vertauscht, so kann z. B. mit Hilfe einer Dummykarte als beweglichen eine echte Schreib-Lesestation zur Ausgabe des zur eingegebenen Information zugehörigen gesuchten Kryptogramms veranlaßt werden.

Die Verwendung eines Globalschlüssels auf der Prüfstellenseite schützt hier nicht, da der dann von der Karte auszugebende Identifikator ID oder CID, der das verschlüsselte Geheimnis enthält, von der Karte vor der Authentifikation ausgegeben werden muß und damit einem Angreifer zugänglich ist.

Bei dem erfindungsgemäßen Verfahren erfolgt der Ablauf daher in folgenden Schritten:

Da das Geheimnis auf beiden Seiten, gegebenenfalls nach Übermittlung des Identifikators bekannt ist, besteht die Möglichkeit einer gleichzeitigen Berechnung der Authentifikationskryptogramme. So kann z.B. die stationäre Station ST eine Zufallszahl R1 generieren und diese an den beweglichen Datenträger BT senden. Der bewegliche Datenträger BT empfängt die Zufallszahl R1 und generiert und sendet eine zweite Zufallszahl R2 an ST und beide, beweglicher Datenträger BT und stationäre Station ST, verschlüsseln beide Zufallszahlen R1, R2 mit einem Geheimschlüssel GS. Das so erhaltene Kryptogramm wird sowohl vom beweglichen Datenträger BT wie auch von der stationären Station ST in mehrere beliebige Teile unterteilt. Dies kann soweit gehen, daß das Kryptogramm in seine einzelnen Bits unterteilt wird. Der bewegliche Teil BT sendet dann den ersten Teil des Kryptogramms von der Zufallszahl R1 an die stationäre Station. Die stationäre Station ST empfängt den ersten Teil des Kryptogramms von R1 und vergleicht diesen mit dem eigenen Kryptogrammteil von R1. Daraufhin sendet die stationäre Station ST den ersten Teil des Kryptogramms von R2 an den beweglichen Datenträger BT. Der bewegliche Datenträger BT empfängt den ersten Teil des Kryptogramms von R2 und vergleicht diesen mit dem eigenen Kryptogrammteil von R2. Daraufhin wiederholt sich der Vorgang mit den jeweiligen anderen Teilen des Kryptogramms.

Bei Nichtübereinstimmung der zu vergleichenden Informationsschritte wird in geeigneter Weise die weitere Ausgabe des Kryptogramms gesperrt. Da beim Fälschungsversuch bereits das erste oder die ersten Bits der Autentifikation nicht übereinstimmen, ist abhängig von der gewählten Schrittzahl die Ausgabe des jeweiligen Teils eines Kryptogramms für einen Betrüger kaum von Nutzen.

Der Anfangsschritt kann sowohl von der stationären Station als auch von der beweglichen Datenträger ausgehen und wird vom wahrscheinlichsten Bedrohungsfalls bestimmt. Der Vorgang kann mit einem Fehlerzähler auch zur endgültigen Sperrung der Karte kombiniert werden.

Desweiteren kann vorgesehen sein, daß bei Abbruch des Authentifikationsvorgangs weiterhin Zufallsfolgen ausgegeben werden, so daß die Abbruchstelle im Bitstrom von außen nicht feststellbar ist.

Patentansprüche

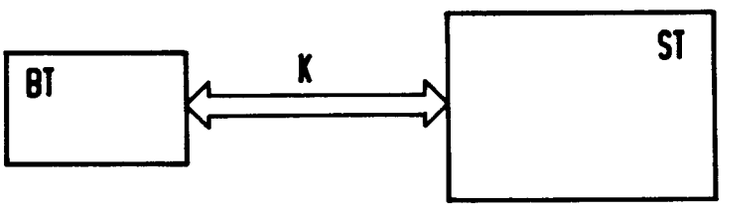
1. Verfahren zur Authentifikation zwischen zwei elektronischen Einrichtungen, **gekennzeichnet durch** die Schritte:
   a) Generieren wenigstens zweier Zufallszahlen,
   b) Übermitteln der beiden Zufallszahlen, so daß beide sowohl in der ersten als auch in der zweiten Station verfügbar sind,
   c) Verschlüsselung der Zufallszahlen in beiden Stationen zu jeweils einen jeder Zufallszahl zugehörigen Kryptogramm,
   d) Übersenden eines Teils des ersten Kryptogramms von einer Station an die andere Station,
   e) Vergleich des Kryptogrammteils in der anderen Station und bei Nichtübereinstimmung Abbruch der weiteren Ausgabe des Kryptogramms,
   f) Übersenden eines Teils des zweiten Kryptogramms von der anderen Station,
   g) Vergleich des von der anderen Station gesendeten Kryptogrammteils in der einen Station und Abbruch des weitere Ausgabe des Kryptogramms bei Nichtübereinstimmung,
   h) Wiederholung der Schritte d) bis g) mit den weiteren Teilen des Kryptogramms bis vollständige Übereinstimmung vorliegt oder Abbruch erfolgte.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet**, daß die eine Zufallszahl in der einen Station erzeugt und in die andere gesendet wird und die andere Zufallszahl in der anderen Station erzeugt und die eine gesendet wird.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet**, daß bei Abbruch des Authentifikationsvorgangs intern beide Stationen Zufallsfolgen weiter nach außen ausgeben, so daß die Abbruchstelle im Bitstrom außen nicht feststellbar ist.

4. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, daß die eine Station eine tragbare Datenträger, insbesondere eine Chipkarte, und die andere Station eine Schreib-Lesestation ist.

5. Verfahren nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet**, daß der tragbare Datenträger einen Fehlerzähler aufweist und daß bei einer vorbestimmten Anzahl von Fehlern die Karte gesperrt wird.


BT
K
ST